UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,067	05/02/2006	Maarten Peter Bodlaender	NL 031313	4777

24737 7590 01/23/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
BROMELL, ALEXANDRIA Y	
ART UNIT	**PAPER NUMBER**
2167	

MAIL DATE	DELIVERY MODE
01/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/578,067	BODLAENDER, MAARTEN PETER	
	Examiner	Art Unit	
	Alexandria Y. Bromell	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 May 2006* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to Applicant's application 10578067, filed 05/02/06. Claims 1-19, which are currently pending, are fully considered below.

Priority

This application is a 371 of PCT/IB04/52233, filed 10/28/04, which claims priority to foreign document EPO 03104086.8, filed 11/05/03.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-12 are rejected because the claims are rejected as falling under the judicial exception of an abstract idea which lacks a useful, concrete, and tangible result. A claimed series of steps or acts that do not result in a useful, concrete, and tangible result are not statutory within the meaning of 35 USC 101. In the instant case, the claims recite, "creating a control point," and "accessing services." However, no useful, concrete, and tangible result is claimed. For example, "writing said data," "updating said data," "sending said data" being claimed at the end of the claim may comprise a useful, concrete, and tangible result. Absent such a result, however, the claims are not statutory.

Claims 13-19 are rejected because the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are nonstatutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Masuouka et al. (U.S. Patent Publication 20050138410) and further in view of Eytchison (WO 01/50290).

With respect to claim 1, Masuouka teaches generating a control point identity for the user based on a public key associated with the user (i.e. a control point identity is generated as a user requests and receives credentials to access a system, where the credentials may be based on public, or shared keys, [0074]), providing at least basic control point functionalities (i.e. while the users credentials remain valid, the user may access the system functions, [0075]), and such that the user can operate any device he is allowed to in the computing environment from any physical entity where the control point is enabled (i.e. user is granted physical access to any device where authentication

is validated, [0044]). Masuouka does not explicitly disclose where the control point is stored. However, Eytchison teaches storing the control point identity and the functionalities as a control point (i.e. server stores policy statements, or information about the user and their functionalities, (page 11)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 2, Masuouka teaches how a user is granted access to a device ([0014). Masuouka does not explicitly disclose that a control point is stored on a server. However, Eytchison teaches the control point is stored on a server that an entity through which a user can access a device can reach (i.e. server stores policy statements, or information about the user and their access to devices in the system, and for controlling the devices, (page 11)). Therefore, the limitations of claim 2 are rejected in the analysis of claim 1 above, and the claim is rejected on that basis.

With respect to claim 3, Masuouka teaches the control point is stored on a smart card of the user (i.e. control point is stored on a smart card or token, [0066]).

With respect to claim 4, Masuouka teaches a replica of the control point is stored in each device the user can be allowed to control (i.e. control point information, like certificates and keys, may be installed on the device, [0074]).

With respect to claim 5, Masuouka teaches the connectivity model is Universal Plug and Play (i.e. Universal Plug and Play (UPnP) networks control the client devices, [0142]).

With respect to claim 6, Masuouka teaches identifying a user wanting to access services at a point of access for the user to the computing environment by using a control point identifier (i.e. user requests access to the environment using a control point identifier, or pin, [0014]), determining if there is a control point associated with the user existing at the point of access (i.e. system determines if pin and user are valid for the point of access, [0156]). Masuouka does not explicitly disclose how a control point is registered on a security console. However, Eytchison teaches copying, if there is no such control point at the point of access, the control point to the point of access (i.e. if user has not already set up a profile, request will be sent for services (page 14)), activating the control point (i.e. system grants service request if all needed information is available, and the resource manager will automatically configure the devices of the network accordingly, (page 14)), and connecting the control point with a device, such that the user can access services from the device in dependence of the fights granted to him (i.e. user will be allowed access to the devices to which he has privilege, (page 14)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the

time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 7, Masuouka teaches the step of identifying comprises performing authentication of the user using the public key and a secret key of the user (i.e. authentification requires public and private keys, [0046]).

With respect to claim 8, Masuouka teaches how a user is granted access to a device ([0014). Masuouka does not explicitly disclose copying a control point. However, Eytchison teaches the step of copying comprises copying the control point from a known user control point store (i.e. profile can be copied from home server system, page 13). Therefore, the limitations of claim 8 are rejected in the analysis of claim 6 above, and the claim is rejected on that basis.

With respect to claim 9, Masuouka teaches how a user is granted access to a device ([0014). Masuouka does not explicitly disclose how a control point is registered on a security console. However, Eytchison teaches registering the control point at a security console using the control point identifier (i.e. control point access information is stored in the access control manager (ACM) to determine the identifier of the user, (page 14)), and granting permission to the control point regarding at least one device

from the security console, such that a user can access services of the device via the control point (i.e. the access control manager enables access for the user to the devices based on user control point privileges, (page 14)). Therefore, the limitations of claim 9 are rejected in the analysis of claim 6 above, and the claim is rejected on that basis.

With respect to claim 10, Masuouka teaches how a user is granted access to a device ([0014). Masuouka does not explicitly disclose that access permissions are determined by an access control list. However, Eytchison teaches the step of granting permission comprises storing the control point identifier in an action control list associated with the device in question (i.e. granting permissions may be facilitated by an access control manager, which has profiles stored with their approved access levels, (page 13)). Therefore, the limitations of claim 10 are rejected in the analysis of claim 9 above, and the claim is rejected on that basis.

With respect to claim 11, Masuouka teaches the step of granting permission comprises providing the control point with a ticket to be used for accessing services of the device (i.e. to grant access to the system, a ticket, or pin is used, [0046]).

With respect to claim 12, Masuouka teaches how a user is granted access to a device ([0014). Masuouka does not explicitly disclose that the security console determines the access rights. However, Eytchison teaches the step of accessing the services using access rights provided by a security console (i.e. user accesses devices based on access rights stored in the access control, or security manager, (page 14)). Therefore, the limitations of claim 12 are rejected in the analysis of claim 9 above, and the claim is rejected on that basis.

With respect to claim 13, Masuouka teaches generate a control point identity for the user based on a public key associated with the user (i.e. a control point identity is generated as a user requests and receives credentials to access a system, where the credentials may be based on public, or shared keys, [0074]), provide at least basic control point functionalities (i.e. while the users credentials remain valid, the user may access the system functions, [0075]), and such that the user can operate any device he is allowed to in the computing environment from any physical entity where the control point is enabled (i.e. user is granted physical access to any device where authentication is validated, [0044]). Masuouka does not explicitly disclose where the control point is stored. However, Eytchison teaches store the control point identity and the functionalities as a control point (30) (i.e. server stores policy statements, or information about the user and their functionalities, (page 11)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 14, Masuouka teaches identify a user wanting to access services at a point of access (12) for the user to the computing environment by using a control point identifier (i.e. user requests access to the environment using a control point identifier, or pin, [0014]), determine if there is a control point (30) associated with the user existing at the point of access (i.e. system determines if pin and user are valid for the point of access, [0156]). Masuouka does not explicitly disclose how a control point is registered on a security console. However, Eytchison teaches copy, if there is no such control point at the point of access, the control point to the point of access (i.e. if user has not already set up a profile, request will be sent for services (page 14)), activate the control point (i.e. system grants service request if all needed information is available, and the resource manager will automatically configure the devices of the network accordingly, (page 14)), and connect the control point with a device (38), such that the user can access services from the device in dependence of the rights granted to him (i.e. user will be allowed access to the devices to which he has privilege, (page 14)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic

devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 15, Masuouka teaches generate a control point identity for the user based on a public key associated with the user (i.e. a control point identity is generated as a user requests and receives credentials to access a system, where the credentials may be based on public, or shared keys, [0074]), provide at least basic control point functionalities (i.e. while the users credentials remain valid, the user may access the system functions, [0075]), such that the user can operate any device (38) he is allowed to in the computing environment from any physical entity (12, 18, 20, 22) where the control point is enabled (i.e. user is granted physical access to any device where authentication is validated, [0044]), identify a user wanting to access services at a point of access (12) for the user to the computing environment by using a control point identifier (i.e. user requests access to the environment using a control point identifier, or pin, [0014]), determine if there is a control point associated with the user existing at the point of access (i.e. system determines if pin and user are valid for the point of access, [0156]). Masuouka does not explicitly disclose where the control point is stored. However, Eytchison teaches store the control point identity and the functionalities as a control point (30) (i.e. server stores policy statements, or information about the user and their functionalities, (page 11)), copy, if there is no such control point at the point of access, the control point to the point of access (i.e. if user has not already set up a profile, request will be sent for services (page 14)), activate the control point (i.e. system grants service request if all needed information is available, and the resource manager

will automatically configure the devices of the network accordingly, (page 14)), and connect the control point with a device (38), such that the user can access services from the device in dependence of the rights granted to him (i.e. user will be allowed access to the devices to which he has privilege, (page 14)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 16, Masuouka teaches computer program code means, to make the computer execute, when said program is loaded in the computer (claim 26), generate a control point identity for the user based on a public key associated with the user (i.e. a control point identity is generated as a user requests and receives credentials to access a system, where the credentials may be based on public, or shared keys, [0074]), provide at least basic control point functionalities (i.e. while the users credentials remain valid, the user may access the system functions, [0075]), and such that the user can operate any device he is allowed to in the computing environment from any physical entity where the control point is enabled (i.e. user is

granted physical access to any device where authentication is validated, [0044]). Masuouka does not explicitly disclose where the control point is stored. However, Eytchison teaches store the control point identity and the functionalities as a control point (i.e. server stores policy statements, or information about the user and their functionalities, (page 11). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 17, Masuouka teaches identify a user wanting to access services at a point of access for the user to the computing environment by using a control point identifier (i.e. user requests access to the environment using a control point identifier, or pin, [0014]), determine if there is a control point associated with the user existing at the point of access (i.e. system determines if pin and user are valid for the point of access, [0156]). Masuouka does not explicitly disclose how a control point is registered on a security console. However, Eytchison teaches computer program code means, to make the computer execute, when said program is loaded in the computer

(claim 26), copy, if there is no such control point at the point of access, the control point to the point of access (i.e. if user has not already set up a profile, request will be sent for services (page 14)), activate the control point (i.e. system grants service request if all needed information is available, and the resource manager will automatically configure the devices of the network accordingly, (page 14)), and connect the control point with a device, such that the user earl access services from the device in dependence of the rights granted to him (i.e. user will be allowed access to the devices to which he has privilege, (page 14)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 18, Masuouka teaches computer program code means, to make the computer execute, when said program element is loaded in the computer (claim 26), generate a control point identity for the user based on a public key associated with the user (i.e. a control point identity is generated as a user requests and

receives credentials to access a system, where the credentials may be based on public, or shared keys, [0074]), provide at least basic control point functionalities (i.e. while the users credentials remain valid, the user may access the system functions, [0075]), and such that the user can operate any device he is allowed to in the computing environment from any physical entity where the control point is enabled (i.e. user is granted physical access to any device where authentication is validated, [0044]). Masuouka does not explicitly disclose where the control point is stored. However, Eytchison teaches store the control point identity and the functionalities as a control point (i.e. server stores policy statements, or information about the user and their functionalities, (page 11)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

With respect to claim 19, Masuouka teaches identify a user wanting to access services at a point of access for the user to 15 the computing environment by using a control point identifier (i.e. user requests access to the environment using a control point

identifier, or pin, [0014]), determine if there is a control point associated with the user existing at the point of access (i.e. system determines if pin and user are valid for the point of access, [0156]). Masuouka does not explicitly disclose how a control point is registered on a security console. However, Eytchison teaches computer program code means, to make the computer execute, when said program element is loaded in the computer (claim 26), copy, if there is no such control point at the point of access, the control point to the point of access (i.e. if user has not already set up a profile, request will be sent for services (page 14)), activate the control point (i.e. system grants service request if all needed information is available, and the resource manager will automatically configure the devices of the network accordingly, (page 14)), and connect the control point with a device, such that the user can access services from the device in dependence of the rights granted to him (i.e. user will be allowed access to the devices to which he has privilege, (page 14)). Masuouka and Eytchison are analogous art because they are from the same field of endeavor of allowing a user to access devices based on access permissions. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Masuouka and Eytchison before him or her, to modify the system of Masuouka with the teachings of Eytchison in order to protect devices from access by unauthorized users (Eytchison, page 3). The motivation for doing so would have been to add a user-dependent access control system for a network of electronic devices (Eytchison, page 3). Therefore, it would have been obvious to combine Eytchison with Masuouka to obtain the invention as specified in the instant claim(s).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Alexandria Y. Bromell whose telephone number is 571-270-3034. The examiner can normally be reached on M-R 6:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mohammad Ali can be reached on 571-272-4105. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Alexandria Y Bromell
Examiner
Art Unit 2169

AYB
January 2, 2008

MOHAMMAD ALI
SUPERVISORY PATENT EXAMINER